CLAIMS

1. (Amended) A method of calculating a value of a given function by using an apparatus including a plurality of computers, comprising:

an input process;

a calculation of each cycle; and

an output process,

characterized in that the input process inputs information describing a construction of a circuit corresponding to the given function and an input bit to the circuit to the plurality of computers, and

in the calculation of each cycle, one of the computers firstly performs calculation and transmits the calculation result to another computer and the another computer which has received the calculation result performs the next calculation such that calculation is performed by one computer after another, and when all the computers have performed calculation once, the last computer which has performed calculation transmits the calculation result to the first computer which has performed calculation, and after this, calculation is performed by one computer after another and the calculation result is transmitted to the next computer such that the calculation of each cycle is repeated.

2. (Amended) A method of calculating a value of a given function by using an apparatus including a plurality of computers, comprising:

an input process;

an ElGamal cipher text preparation process;

a sequential substitution reencryption process; and

a result output process,

characterized in that the input process comprises an information input step of inputting to the plurality of computers information on a circuit including a plurality of gates and information on the plurality of computers, and a dispersion input step of inputting to each of the computers each one of plural pieces of partial data which are obtained by dispersing input data of the function into plural pieces by the number of the computers,

the ElGamal cipher text preparation process comprises an ElGamal cipher text preparation step of generating a set of ElGamal cipher texts in which at least one of the computers corresponds to the gate of the circuit that realizes the given function,

the sequential substitution reencryption process comprises a step of allowing each of the computers to perform a substitution reencryption process one after another, and the substitution reencryption process comprises a cipher text obtaining step of allowing the computer in this turn to receive the set of ElGamal cipher texts from the computer in the previous turn, a cipher text substitution and reencryption step of changing an order of the set of cipher texts received in the cipher text obtaining step for substitution and subjecting those cipher texts to reencryption, and a step of disclosing the data generated in the cipher text substitution and reencryption step to at least the computer in the next order,

the result output process comprises a partial decryption step of deciphering or partially deciphering a part of the cipher texts generated in the cipher text substitution and reencryption step, a decryption step of deciphering a cipher text that enciphers data corresponding to the input to the circuit in the cipher texts generated in the cipher text substitution and reencryption step, and an evaluation step of evaluating an output of the circuit by using the data deciphered In the decryption step and the data partially deciphered in the partial decryption step,

the set of ElGamal cipher texts corresponding to each of the gates is a set of ElGamal cipher texts of a secret key generated corresponding to each of the gate by each of the computers,

a public key used for generating the ElGamal cipher texts is a sum of public keys corresponding to gates for generating two signals input to this gate,

a plurality of combinations of a cipher text corresponding to an output "1" and a cipher text corresponding to an output "0" are prepared for logial expressions to be calculated,

a sequential encryption process is a process which subjects the cipher texts to reencryption and substitution, substitutes the ciper texts corresponding to "1" and "0" with each other, and does not substitute the cipher texts corresponding to "1" and "1" with each other, and

the cipher texts of either "1" or "0" is subjected to decryption as a final decryption result.

3. (Amended) A calculation system for evaluating a function, comprising:

a plurality of computers;

communication means for performing communication with the plurality of computers;

input process means;

ElGamal cipher text preparation means;

sequential substitution reencryption means; and

result output means,

characterized in that the input means inputs information on a circuit whose output is desired to be obtained, information on the plurality of computers, and information on which part of an input to the circuit each of the computers has,

the ElGamal cipher text preparation means prepares ElGamal cipher texts for generating a set of ElGamal cipher texts corresponding to gates of the circuit that realizes the given function,

the sequential substitution reencryption means comprises cipher text obtaining means for allowing the computer in this turn to receive the set of ElGamal cipher texts from the computer in the previous turn, cipher text substitution and reencryption means for changing an order of the set of cipher texts received by the cipher text obtaining means for substitution and subjecting those cipher texts to reencryption, and means for disclosing the data generated by the cipher text substitution and reencryption means to at least the computer in the next order, and

the result output means comprises partial decryption means for deciphering or partially deciphering a part of the cipher texts generated by the cipher text substitution and reencryption means, decryption means for deciphering encryption related to itself of a cipher text that enciphers data corresponding to the input to the circuit in the cipher texts generated by the cipher text substitution and reencryption means, and evaluation means for evaluating an output of the circuit while using the data deciphered by the decryption means by the plurality of computers and the data partially deciphered by the partial decryption means by the plurality of computers.

the set of ElGamal cipher texts corresponding to each of the gates is a set of ElGamal cipher texts of a secret key generated corresponding to each of the gate by each of the computers,

a public key used for generating the ElGamal cipher texts is a sum of public keys corresponding to gates for generating two signals input to this gate,

a plurality of combinations of a cipher text corresponding to an output "1" and a cipher text corresponding to an output "0" are prepared for logial expressions to be calculated,

a sequential encryption process is a process which subjects the cipher texts to reencryption and substitution, substitutes the ciper texts corresponding to "1" and "0" with each other, and does not substitute the cipher texts corresponding to "1" and "1" with each other, and the cipher texts of either "1" or "0" is subjected to decryption as a final decryption result.

4. (Deleted)

5. The calculation method according to Claim 2,

characterized in that the input process further comprises a step of inputting an area variable of an ElGamal encryption method to each of the computers,

the ElGamal cipher text preparation process further comprises a gate secret key generating step of generating a secret key of the ElGamal cipher texts corresponding to each of the gates of the circuit by each of the computers,

each of the computers performs:

a gate public key generating step of generating a gate public key corresponding to the secret key generated in the gate secret key generating step;

a gate public key validity proof generating step of generating a gate public key validity proof for the public key generated in the gate public key generating step;

a gate public key validity proof disclosing step of disclosing the gate public key validity proof generated in the gate public key validity proof generating step;

an input gate secret key generating step of generating a secret key of the ElGamal cipher texts corresponding to a gate where an input is directly made to the circuit of the gates of the circuit;

an input gate public key generating step of generating an input gate public key corresponding to the secret key generated in the input gate secret key generating step;